Stand: 24.10.2007

CISCO-Workaround: Forcing the VPN3000 to Generate the Certificate Request in Software

We have come up with a workaround that we'd like the customer to try. The workaround consists of forcing the vpn3000 to generate the certificate request in software. Note that generating the keys in software takes somewhat longer than generating keys in the SEP modules (about 1 - 2 minutes per request).

In order to do this, the SEP modules must be disabled. This can either be done by physically removing the SEPs, or by disabling them via a 911 command. Note that both of these methods will require that the vpn3000 be powered off.

If they are removing the SEPs, the steps are as follows:

1. Power off the vpn3000
2. Remove all SEP modules
3. Power on the vpn3000
4. Generate the certificate request(s) as they normally would
5. Verify the request is "2048" bits
6. Power off the vpn3000
7. Re-insert the SEP modules 8. Power on the vpn3000

To disable the SEPs via a 911 command, the steps are:

1. Log in to the console using the administrator username/password
2. Enter '911' and enter the administrator username/password to enter 911 mode
3. Enter the command "debug 14 11 x", where 'x' is the SEP number. Do this for all installed SEP modules
4. Generate the certificate request(s) as they normally would
5. Verify the request is "2048" bits
6. Power cycle the vpn3000 to re-enable the SEP modules

Note that with either of the above methods, there is still the possibility that the vpn3000 will generate what the customer is calling "2047 bit" keys. These keys are actually 2048 bit keys with the most significant bit cleared. Since keys are created based on a random number, the vpn3000 generates keys with this bit set or cleared approximately 50% of the time. If a "2047" bit key is generated, the customer should try again until a key is generated that has the most significant bit set.

In the meantime, we will continue to investigate why the vpn3000 hardware only generates keys with the first bit cleared.